# Official CalPSAB Security Guidelines (Final)

***All Guidelines Approved by CalPSAB (Advisory Board)***

## 1 – Administrative Controls

### (a) Information Security (Organization & Responsibility)

An entity shall identify the entity's primary security official who is responsible for implementation and compliance to these guidelines. Such official shall be identified in such a way that anyone who might have a security issue or concern may contact that person.

*[45 C.F.R § 164.308 (a)(2)]*

#### *(1) Responsibility & Coordination of Information Security Assets*

An entity shall account for information security assets and designate the asset owner(s). Appropriate security controls shall be assigned for each class or group of information security assets. Implementation of specific controls may be delegated by the owner as appropriate. The owner remains responsible for the proper protection of the assets in all cases where delegation occurs.

*[ISO 7.1 Responsibility for Assets]*

#### *(2) Information Security Policy Approvals & Management*

An entity shall comply with the following:

In deciding which security measures to use, an entity shall, at a minimum, take into account the following factors:

(i) The size, complexity, and capabilities of the entity.

(ii) The entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs/benefits of security measures.

(iv) The probability and criticality of potential risks to individual health information.

This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of these guidelines.

*[45 C.F.R § 164.316 (a)]*

#### *(3) Applications Inventory*

An entity shall identify all operating, database, and application assets (e.g. application software, system software, development tools) that support the exchange

and processing of individual health information and document the importance of these assets. An application inventory shall include all information necessary in order to recover from a disaster or other business interruption, such as, but not limited to, application logging, type of asset, format, location, backup information, license information, and business value. See also: Guideline 2(a)(2) – Recovery Strategies.

*[45 C.F.R. § 164.308 (7)(ii)(E), ISO 7.1.1 Inventory of Assets]*

### *(4) Isolating Health Care Clearinghouse Functions*

If a health care transaction clearinghouse is part of a larger entity, the clearinghouse segment shall protect and isolate individual health information of the clearinghouse from unauthorized access by the larger organization.

*[45 C.F.R. § 164.308 (a)(4)(ii)(A)]*

## (b) Risk Management Program

An entity shall develop and implement a risk management program that enables the entity to assess and reduce risk to an acceptable level.

*[45 C.F.R. § 164.308 (a)(1)(i)]*

### *(1) Risk Assessment*

An entity shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of individual health information held, created, processed, transmitted or received by an entity.

*[45 C.F.R. § 164.308 (a)(1)(ii)(A)]*

### *(2) Risk Management & Mitigation*

An entity shall implement security measures sufficient to reduce risks and vulnerabilities to:

***(i)*** Protect the confidentiality, integrity, and availability of all individual health information the entity creates, receives, maintains, or transmits.

***(ii)*** Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

***(iii)*** Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under these guidelines.

***(iv)*** Take steps to ensure compliance with these guidelines by its workforce.

*[45 C.F.R. §§ 164.308 (a)(1)(ii)(B) & 164.306 (a)]*

## (c)Workforce Security Management

With regard to managing sensitive data, an entity shall ensure that all members of its workforce have appropriate access to individual health information and prevent workforce members from obtaining unauthorized access to individual health information.

*[45 C.F.R. § 164.308 (a)(3)(i)]*

### *(1) Workforce Supervision*

An entity shall establish a process for authorizing and managing access provisioning and controls for workforce members. An entity shall supervise workforce members. At minimum, an entity shall supervise workforce members by employing the following guiding principles:

(i) Least privilege

(ii) Default to no access

(iii) Review and adjust privilege, if needed, upon change of job duties or other changes that impact the need for access

(iv) Promptly remove access to individual health information when access is no longer required

(v) Periodic review of workforce access privileges

*[45 C.F.R. § 164.308 (a)(3)(ii)(A)]*

### *(2) Workforce Sanctions & Accountability*

An entity shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the entity.

*[45 C.F.R. § 164.308 (a)(1)(ii)(C)]*

### *(3) Permitted Use of Equipment*

An entity shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation, including but not limited to, mobile electronic computing devices that can access individual health information.

*[45 C.F.R. § 164.310 (b)]*

## (d) Compliance Testing, Audit & Monitoring

An entity shall take steps to ensure compliance of their systems with these security guidelines. The security of information systems shall be regularly reviewed. Such reviews shall be performed against these guidelines.

If any non-compliance is found as a result of the review, managers shall, at a minimum:

(i) Determine the causes of the non-compliance

(ii) Remediate issues found to cause non-compliance, or management shall respond indicating why this risk was accepted or not applicable

(iii) Evaluate the effectiveness of the corrective action, post-implementation

*[ISO 15.2 Compliance with Security Policies and Standards, and Technical Compliance]*

### *a) Activity Review & Monitoring (Logs)*

An entity shall regularly review records of activity and monitor information systems that contain IHI. Review information security controls (such as audit logs, access reports, and security incident tracking reports) for indications of control failure or exploitation of information systems. An entity shall take actions to remediate, as appropriate.

*[45 C.F.R. § 164.308 (a)(1)(ii)(D)]*

### *b) Evaluation of Policy and Technical Compliance*

An entity shall perform and document a technical and non-technical evaluation on an iterative basis that demonstrates due diligence and an active evaluation program. Iterative reviews should be performed whenever environmental, operational, or technical changes occur that may introduce security vulnerabilities.

*[45 C.F.R. § 164.308 (a)(8)]*

## (e) Security Incident Management Response, & Documentation

An entity shall address security incidents. An entity shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes. An entity shall take measures necessary to determine the scope of the breach and correct offending deficiencies in security controls to prevent a recurrence of the breach of the information system.

*[45 C.F.R. §§ 164.308 (a)(6)(ii), California Civil Code § 1798.82(a)]*

## (f) Frequency of Actions

Activities required by these guidelines shall be performed at a frequency determined by an entity based on knowledge of activities and/or changes within the organization, or as required by other legal or contractual obligations.

*[CalPSAB ]*

# 2 – Business Continuity & Contingency Planning

## (a) Contingency Planning

An entity shall document a comprehensive business continuity plan and recovery strategies including elements related to people, processes, environment, incident management, and coordination with emergency response, crisis communications, and individual health information data. Such a plan should include a listing of identified risks and mitigation or acceptance statements for each risk. (Note: See Guideline Policy 5.2 Risk Management Program).

Entities implementing operations subject to these guidelines are responsible for understanding and being compliant with applicable federal, state and local legislation and regulatory requirements related to business continuity planning.

*[CalPSAB ]*

### *(1) Business Impact Analysis*

An entity shall document a Business Impact Analysis that identifies any vulnerability and develop strategies for minimizing risk. The Analysis should describe the potential risks specific to the entity and all critical business components.

The BIA shall include, but is not limited to:

(i) Applications & Data Criticality Analysis
(ii) Change Management

*[CalPSAB ]*

### (2) Recovery Strategies

An entity shall document strategies for business recovery from a serious disruptive event. The recovery strategies should define procedures to be followed to achieve a structured and coherent recovery process. The entity shall review any pre-defined procedures in the event of an actual situation arising following a disruptive event and modify these procedures as appropriate.

Defined procedures should include, but are not limited to:

- Incident Management
- Emergency Response
- Crisis Communications
- Disaster Recovery Plan, to include:
    - Technical Recovery Plans
    - Facilities
    - Business Recovery Plans

*[CalPSAB ]*

### (3) Business Continuity Plan

An entity shall implement a Business Continuity Plan that details procedures and processes for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages, or makes

inaccessible, systems that contain individual health information. Consideration should be given to multi-system approach, inter-disciplines, all locations where IHI resides, and all business process boundaries (interface points).

The Continuity Plan shall include, but is not limited to:

- Business Impact Analysis (BIA)
- Recovery Strategies
- Testing and Revision of the Continuity Plan

*[CalPSAB ]*

### (4) Testing & Revision of Continuity Plan

An entity shall create and maintain applications/systems to protect the integrity and availability of individual health information.

An entity shall periodically test and revise their contingency plan.

*[45 C.F.R. § 164.308 (a)(7)(ii)(D)]*

## 3 – Facility & Equipment Controls

### (a) Facility Access Controls

An entity shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

*[45 C.F.R. § 164.310 (a)(1)]*

### (1) Physical Access Management

An entity shall safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft, including procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

An entity shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)

*[45 C.F.R. §§§ 164.310 (a)(2)(ii) & 164.310 (a)(2)(iii) & 164.310 (a)(2)(iv)]*

### (2) Communications & Operations Management

An entity shall assign responsibilities for the management and operation of all information processing facilities that handle individual health information.

An entity shall establish formal exchange policies, procedures, and controls to protect the exchange of information through the use of all types of communication facilities.

*[ ISO 10.1 Operational Procedures and Responsibilities, 10.8 Exchange of Information]*

## (b) Device & Media Controls

An entity shall control, administer and maintain a record of the consignment of hardware and electronic media that contain individual health information and any person responsible therefore and maintain the inventory of such assets.

*[45 C.F.R. § 164.310 (d)(1)]*

### (1) Mobile Electronic Device Controls

An entity shall limit and protect the storage of Individual Health Information (IHI) on mobile electronic computing devices and passive storage media. Storage of IHI on mobile electronic computing devices and passive storage media is prohibited unless the devices or IHI:

- Are physically secured in accordance with CalPSAB Security Guidelines
- Are encrypted where indicated by risk assessment, using minimum encryption standards identified in the CalPSAB Security Guidelines. See Security Guideline 8.1.2 Encryption and Cryptographic Controls
- Note: Legacy medical devices may require alternative controls in lieu of standard controls as allowed by device manufacturers, such deviations from standard controls shall be documented

An entity shall have a policy directing all workforce members, using any non-managed (user-owned) devices or media, to adhere to the user's entity requirements identified in these guidelines.

### (2) Unsecured IHI Loss Prevention *(moved from (3)d2))*

An entity shall take reasonable steps to prevent the unauthorized removal or transmission of individual health information, including but not limited to, data leakage, laptop or flash drive loss, etc.

*[Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages 19006-19010]*

### (3) Workstation & Security Equipment Controls

An entity shall implement physical and/or technical safeguards for all workstations that access individual health information, to restrict access to authorized users.

*[45 C.F.R. § 164.310 (c)]*

### (4) Reuse of Media

An entity shall implement procedures for removal of individual health information from electronic media before the media is made available for re-use.

*[45 C.F.R. § 164.310 (d)(2)(ii)]*

### (5) Disposal of Media

An entity shall utilize a method that best meets the entity's business practices and protects the security of individual health information for final disposition of individual health information, hardware, and/or electronic media on which the individual health information is stored.

The media on which the IHI is stored or recorded have been destroyed in one of the following ways:

- Paper, film, or other hard copy media have been shredded or destroyed such that the IHI cannot be read or reconstructed. Redaction is specifically excluded as a means of data destruction.
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization.

*[45 C.F.R. § 164.310 (d)(2)(i), Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages 19006-19010]*

## (c)Technical Controls

An entity shall protect individual health information in information systems as specified in the guidelines.

*[45 C.F.R. § 164.312(a)]*

### (1) Login Monitoring

An entity shall monitor log-in attempts, reporting discrepancies, and take actions to remediate, as appropriate.

*[45 C.F.R. § 164.308 (a)(5)(ii)(C)]*

### (2) Operating System & Database Hardening / Patch Management

As appropriate, an entity shall comply with the following for the protection of individual health information:

- Apply patches or use other appropriate mechanisms (e.g., update the operating system (OS) and databases) on a timely basis
- Harden and configure the OS and databases to address security vulnerabilities
- Install and configure necessary security controls
- Regularly test the security of the OS and databases to ensure that the previous steps address known security issues

*[NIST SP 800-123 (Section 4) – Securing the Server Operating System]*

### (3) Malicious Code Protection

An entity shall take appropriate steps to protect against malicious software. In addition, an entity shall incorporate a mechanism to detect, mitigate and immediately report malicious software to the primary security official or designee for response if necessary.

*[45 C.F.R. § 164.308 (a)(5)(ii)(B)]*

### (4) Email & Messaging Security

An entity shall safeguard electronic mail and messaging containing individual health information in its possession.

*[NIST SP 800-45 v2 Guidelines on Electronic Mail Security, ISO 10.8.4 Electronic Messaging]*

### (5) Audit Controls

An entity shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use individual health information.

*[45 C.F.R. § 164.312 (b)]*

## (d) Network Security Management

An entity shall protect the networks and infrastructures that maintain or transmit individual health information.

*[ISO 10.6 Network Security Management]*

### (1) Perimeter Controls & Management

An entity shall identify and include, or reference, security features, service levels, and management requirements of all network services in any network services agreement, whether these services are provided in-house or outsourced. Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and a system to detect intrusion.

*[ISO 10.6.2 Security of Network Services]*

### (2) Intrusion Detection

An entity shall implement an internal system to detect intrusion attempts. The entity shall document and report successful intrusions to the primary security official or designee for response.

*[NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)]*

### (3) Consistent Time

An entity shall take steps to ensure clocks of all relevant information processing systems within an organization are synchronized using an accurate reference time source using the Network Time Protocol (NTP).

*[CalPSAB]*

# 4 – Data Protection & User Access Controls

## (a) Access Controls

An entity shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.

*[45 C.F.R. § 164.312 (a)]*

### (1) Identity Management (Internal)

An entity shall establish policies and procedures to verify the identity of workforce members who will access the entity's systems. An entity shall, at a minimum:

- Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations).
- Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization.
- Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role.
- Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

*[45 C.F.R. § 164.514(h) and 164.530(i), NIST SP 800-63 (Section 6.3.1) Requirements per Assurance Level, ISO 11.2 User Access Management]*

### (2) Single Entity Authentication (Non-Federated)

An entity shall authenticate each authorized user's identity prior to providing access to individual health information.

An entity shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to individual health information is the one claimed.

An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity.

An entity shall authenticate users attempting to access individually identifiable health information from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [*See NIST SP 800-63 Rev-1*]

*[45 C.F.R. §§ 164.312 (a)(2)(i) & 164.312 (d), NIST SP 800-63 Rev 1 Electronic Authentication Guideline, OMB Safeguarding Against and Responding to the Breach of Personally Identifiable Information M 07-16]*

## (3) Authentication Across Multiple Entities (Federated)

If an entity is participating in a trust network HIE:

- The trust network shall manage entity authentication for those participating on the trust network, and
- An entity shall manage user authentication only for those entities participating on the trust network.

If the user authentication process is across multiple systems or entities, an entity shall implement the agreed upon authentication process among the participants in the trust network.

An entity participating in the trust network shall implement a trust agreement. *[See Guideline 4.9 Contracts and Agreements]*

> *For example, an entity may use an Interconnections Security Agreement (ISA) and Memorandum of Understanding (MOU) in accordance with NIST SP 800-47 Federal Security Guide for Interconnecting Information Technology Systems, unless such requirement has been superseded by implementation of the national Data Use and Reciprocal Support Agreement (DURSA).*

The entity shall adopt an authentication solution that incorporates the authorization requirement of these guidelines. See Guideline 8.1.4 (v3) *Authorization & Access Control*.

*[CalPSAB]*

## (4) Authorization & Access Control

An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with state requirements:

(1) Data Source;

(2) Entity of Requestor;

(3) Role of Requestor;

(4) Use of Data;

(5) Sensitivity of Data;

(6) Consent Directives of the Data Subject

An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.

*[CalPSAB]*

### (5) Password Management

Where an entity uses password authentication, it shall require passwords to be created, changed periodically, safeguarded, and of sufficient length and complexity to protect individual health information.

- Note: As applicable, passwords shall be used for all mobile electronic computing devices and passive storage media that contain IHI.

*[45 C.F.R. § 164.308 (a)(5)(ii)(D)]*

### (6) Session Controls

An entity shall implement procedures and technical controls to protect against the unauthorized access to individual health information via workstations, which can include, but are not limited to:

- Setting session timeout due to inactivity
- Password protection for locking screens
- Lockout based on unsuccessful logon attempts
- Turn on access (security event) logs and regularly review
- Limit physical access to workstations

*[45 C.F.R. § 164.312 (a)(2)(iii)]*

## (b) Data Assurance

An entity shall protect individual health information from unauthorized alteration or destruction.

An entity shall implement technical security measures to guard against unauthorized access to, or modification of, individual health information that is being transmitted over an electronic communications network.

*[45 C.F.R. §§ 164.312 (c)(1) & 164.312 (e)(1)]*

### (1) Encryption & Cryptographic Controls

An entity shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect individual health information. Entities shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or it's successor, should be periodically reviewed for updated information as part of each organizations' internal best practices.

*[45 C.F.R. § 164.312 (a)(2)(iv)], HITECH Breach Notification Law, FTC*

### (2) Integrity Controls

An entity shall implement security measures to safeguard electronically transmitted individual health information from being modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that individual health information has not been altered or destroyed in an unauthorized manner.

*[45 C.F.R. §§ 164.312 (e)(2)(i) & 164.312 (c)(2)]*